논문 2008-45SD-2-8

고속 비트-직렬 유한체 곱셈기

(Fast Bit-Serial Finite Field Multipliers)

장 남 수*, 김 태 현**, 이 옥 석**, 김 창 한***

(Nam Su Chang, Tae-Hyun Kim, Ok Suk Lee, and Chang Han Kim)

요 약

유한체 연산 기반의 암호시스템에서 곱셈 연산은 가장 주된 연산부로 구성된다. 또한 곱셈기 설계 환경의 자원이 제약적인 경우 비트-직렬 구조가 많이 고려된다. 본 논문은 기존의 비트-직렬 곱셈기에 비하여 작은 시간 복잡도를 가지는 삼항 기약 다항식 기반의 유한체 고속 비트-직렬 곱셈기를 제안한다. 제안하는 두 가지 타입의 곱셈기는 기존의 곱셈기에 비하여 시간 복잡도면에서는 모두 효율적이고, Interleaved 곱셈기의 m·MUL+2m·ADD 시간지연 보다 작은 (m+1)·MUL+(m+1)·ADD 시간 지연만으로 수행이 가능하다. 따라서 확장체의 표수가 작은 타원곡선 암호 시스템, 페어링 기반의 암호시스템에서 고속 동작가능하며, 표수가 2 또는 3인 경우 기존의 곱셈기 보다 대략 2배 빠르게 동작한다.

Abstract

In cryptosystems based on finite fields, a modular multiplication operation is the most crucial part of finite field arithmetic. Also, in multipliers with resource constrained environments, bit-serial output structures are used in general. This paper proposes two efficient bit-serial output multipliers with the polynomial basis representation for irreducible trinomials. The proposed multipliers have lower time complexity compared to previous bit-serial output multipliers. One of two proposed multipliers requires the time delay of (m+1)·MUL+(m+1)·ADD which is more efficient than so-called Interleaved Multiplier with the time delay of m·MUL+2m·ADD. Therefore, in elliptic curve cryptosystems and pairing based cryptosystems with small characteristics, the proposed multipliers can result in faster overall computation. For example, if the characteristic of the finite fields used in cryprosystems is small then the proposed multipliers are approximately two times faster than previous ones.

Keywords: Bit-Serial Multiplier, Elliptic Curve Cryptosystem, Pairing Based Cryptosystem, Hardware Architecture

I. 서 론

유한체는 부호이론, 공개키 암호시스템 등에 널리 활용되며, 공개키 암호시스템 중에서 타원곡선 암호시스템(Elliptic Curve Cryptosystem), 페어링 기반의 암호시스템(Pairing Based Cryptosystem) 등은 유한체 연산 중 곱셈 연산을 주된 연산으로 한다. 유한체 연산은 주로 덧셈과 곱셈으로 구성되며, 그 외 지수승, 역원 연산 등은 덧셈과 곱셈의 반복 연산으로 구성된다. 그리고 곱셈 연산은 덧셈 연산에 비하여 시간-공간 자원을 많이 사용한다. 따라서 시스템 설계의 관점에서 효율적인 곱셈기 설계는 매우 중요하다.

유한체 원소의 표현은 곱셈기의 시간-공간 복잡도에 큰 영향을 미친다. 원소 표현을 위한 기저로는 일반적으로 다항식기저, 정규기저, Dual Basis 등이 사용되며, 이중 정규기저의 경우 제곱 연산을 사이클릭 쉬프트(Cyclic Shift) 연산으로 매우 쉽게 처리한다. 그러나 정규기저의 경우 다른 기저에 비하여 곱셈기 설계의 복잡도가 크다는 단점을 가진다. 따라서 본 논문에서는

* 학생회원-주저자, ** 학생회원, 고려대학교 정보경영공학전문대학원
(Graduate School of Information Management and Security, Korea University)
*** 평생회원-교신저자, 세명대학교 정보통신학부
(School of Information & Communication systems, Semyung University)
※ "본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-(C1090-0801-0025))
접수일자: 2007년11월7일, 수정완료일: 2008년1월7일

다항식기저를 사용한 곱셈기에 대하여 논하도록 한다.

공개키 암호시스템에서 유한체 연산의 고속화를 위하여 표수는 2, 3 등 작은 수를 선택하며, 최근 표수가 3인 유한체 위의 초특이 타원곡선에 대한 암호 어플리케이션을 Koblitz[8]와 Galbraith[9]가 제안하였다. 이와 같은 페어링 연산 기반 암호시스템은 모듈러 감산연산의 효율성을 고려하여 삼항 기약다항식을 주로 사용한다.

유한체 곱셈은 하드웨어로 비트-병렬(Bit-Parallel), 비트-직렬(Bit-Serial) 등의 타입으로 설계되며, 비트-병렬 곱셈기에 비하여 적은 자원을 사용하는 비트-직렬 곱셈기의 경우 병렬-출력(Parallel Output) 또는 직렬-출력(Serial Output)으로 나뉜다. 이때 곱셈 방법은 계수를 처리하는 순서에 따라 MSE(Most Significant Element), LSE(Least Significant Element) 타입으로 구분된다[1~7]. 각각의 타입은 적용 환경에 따라 장단점을 가지며 이는 시간-공간 복잡도에 영향을 미친다. LSE 타입의 경우 내부연산 모듈의 일부를 병렬화 할 수 있는장점을 가지지만 레지스터의 증가와 제어부가 복잡해지는 단점을 가진다. 따라서 논문에서는 MSE 타입의 곱셈기에 대하여 논하도록 한다.

본 논문에서는 MSE 타입의 새로운 비트 직렬 곱셈기를 제안한다. 제안하는 곱셈기는 삼항 기약다항식을 기반으로 설계되며, 삼항 기약다항식이 사용되는 페어링 기반의 암호시스템의 GF(3^m)을 예로 설계한다. 제안하는 곱셈기는 기존의 MSE 타입 곱셈기에 비하여 작은 시간지연을 가지며, 표수에 의존하지 않고 적용가능하다. 또한 확장체의 표수가 작은 타원곡선 암호 시스템, 페어링 기반의 암호시스템에서 고속 동작가능하며, 표수가 2 또는 3인 경우 기존의 곱셈기 보다 대략 2배 빠르게 동작한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 기존의 비트-직렬 곱셈기에 대하여 타입 별로 기술한다. Ⅲ장에서는 제안하는 비트-직렬 곱셈기를 기술한다. Ⅳ장에서는 기존의 결과와 제안하는 곱셈기의 효율성을 비교하고 결론을 내린다.

Ⅱ. 기존의 비트-직렬 곱셈기

$f(x)$를 $GF(3)$위에서 차수가 m인 삼항 기약다항식이라 하고 $f(x) = x^m+f_t x^t+f_0$, $f_t, f_0 \in GF(3)$, $t < m/2$라 하자. 그러면 유한체 $GF(3^m)$는 $GF(3)[X]/(f(x))$와 동형이기 때문에 $GF(3^m)$의 원소 $a(x)$는 다항식 기저를 이용해서 다음과 같이 표현할 수 있다.

$$a(x) = a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 = (a_{m-1} \cdots a_1 a_0), \quad a_i \in GF(3).$$

a_i는 $GF(3)$의 원소이기 때문에 a_i를 표현하기 위해서는 2비트가 필요하게 된다. [PS03]에서는 $GF(3)$의 원소를 표현하기 위하여 다음과 같은 표기법을 사용하였다.

$$a_i = (a_i^H, a_i^L), \text{ where } a_i^H = a_i \text{ div } 2 \text{ and } a_i^L = a_i \bmod 2$$

이 표현법을 이용하여 $GF(3)$의 원소 a_i와 b_i의 덧셈 $c_i = a_i + b_i$은 3 XOR 게이트와 4 OR 게이트를 이용하여 다음과 같이 계산된다.

$$c_i^H = (a_i^L \vee b_i^L) \oplus t \text{ and } c_i^L = (a_i^H \vee b_i^H) \oplus t,$$
$$t = (a_i^L \vee b_i^H) \oplus (a_i^H \vee b_i^L)$$

특히 $2(a_i^H, a_i^L) = -(a_i^H, a_i^L) = (a_i^L, a_i^H)$이므로 뺄셈과 2에 의한 곱셈은 덧셈을 이용하여 쉽게 계산할 수 있다.

1. MSE 타입의 비트-직렬 곱셈기

유한체 곱셈은 r'(x)=a(x)·b(x)의 곱셈 연산과 r(x)= r'(x) mod f(x)의 모듈러 연산으로 구분된다. 따라서 MSE 타입의 비트-직렬 곱셈 또한 곱셈과 모듈러 연산을 독립으로 수행하는 곱셈기와 병렬 수행하는 Interleaved 곱셈기로 구분되며 각각은 알고리즘 Algorithm 1, 2와 같다. 본 논문에서는 편의를 위하여 각각을 타입1, 타입2 곱셈기라 정의한다.

타입1의 경우 계수 곱셈과 r'(x)의 덧셈 연산으로 구성되나 GF(3)의 계수 곱셈은 1 또는 -1의 곱셈이므로 반복문은 덧셈 또는 뺄셈 연산을 m번 반복하게 된다. 그리고 모듈러 연산 r(x)=r'(x) mod f(x)는 삼항 기약다항식의 중간 항의 차수 t가 t<m/2를 만족하면 3번의 덧셈 또는 뺄셈 연산으로 구성된다. 따라서 r(x)의 계산에 m+3번의 덧셈 또는 뺄셈으로 r(x)를 계산할 수 있다. 타입 2의 경우

$$r(x) = a_i \cdot b(x) + r(x) \cdot x \mod f(x)$$
$$= a_i \cdot b(x) + r(x) \cdot x - r_{m-1} \cdot f(x)$$

를 반복적으로 수행하며 r(x)는 항상 m개의 항을 가진다. 따라서 2m번의 덧셈 또는 뺄셈으로 r(x)를 계산할 수 있다. 타입1의 경우 빠른 연산 속도를 가지나 r'(x)가 r(x)의 2배의 저장 공간과 추가 모듈러 연산부가 필요하다는 단점을 가지고 있으며, 타입 2의 경우 추가 모듈러 연산 모듈이 필요 없으나 연산속도가 느린 단점

Algorithm 1 MSE 타입의 비트-직렬 곱셈
(곱셈과 모듈러 연산 독립 수행)

Input : $a(x)=\sum_{i=0}^{m-1}a_i x^i,\quad b(x)=\sum_{i=0}^{m-1}b_i x^i,\quad a_i,b_i\in GF(3)$

Output: $r(x)=a(x)\cdot b(x)=\sum_{i=0}^{m-1}r_i x^i,\quad r_i\in GF(3)$

```
r(x) ← 0
for i = m-1 to 0 do
    r'(x) ← a_i·b(x) + r'(x)·x
end for
r(x) ← r'(x) mod f(x)
Return (r(x))
```

Algorithm 2 MSE 타입의 비트-직렬 곱셈
(곱셈과 모듈러 연산 병렬 수행)

Input : $a(x)=\sum_{i=0}^{m-1}a_i x^i,\quad b(x)=\sum_{i=0}^{m-1}b_i x^i,\quad a_i,b_i\in GF(3)$

Output: $r(x)=a(x)\cdot b(x)=\sum_{i=0}^{m-1}r_i x^i,\quad r_i\in GF(3)$

```
r(x) ← 0
for i = m-1 to 0 do
    r'(x) ← a_i·b(x) + r(x)·x
    r(x)  ← r'(x) mod f(x)
end for
Return (r(x))
```

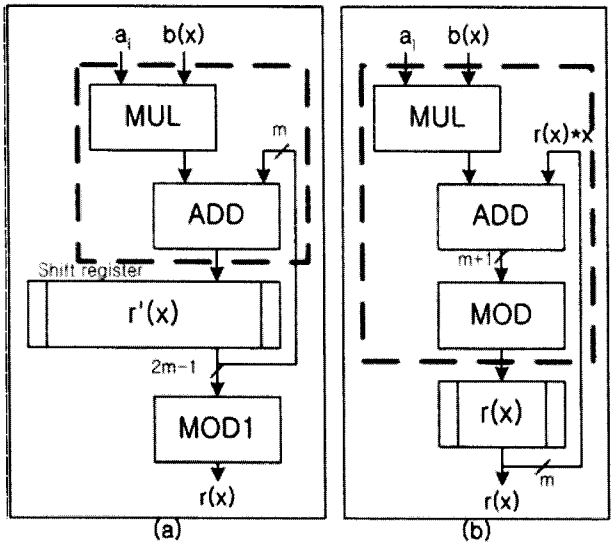


그림 1. 기존의 비트-직렬 곱셈기: (a) 타입 1 (b)타입 2
Fig. 1. Previous Bit-Serial Multiplier: (a) Type 1 (2) Type 2.

을 가진다. 기존의 타입1, 타입2 곱셈기는 그림 1과 같다. 그림 1(a)의 MOD1은 2m-1차 다항식에 대한 모듈러 감산 연산부이며, 점선 박스는 반복 동작이 수행되는 부분을 나타낸다.

III. 제안하는 비트-직렬 곱셈기

본 장에서는 기존의 비트 병렬 곱셈기에 비하여 고속 동작하는 새로운 곱셈기를 제안한다.

Algorithm 3 MSE 타입의 비트-직렬 곱셈
(곱셈과 모듈러 연산 독립 수행)

Input : $a(x)=\sum_{i=0}^{m-1}a_i x^i,\quad b(x)=\sum_{i=0}^{m-1}b_i x^i,\quad a_i,b_i\in GF(3)$

Output: $r(x)=a(x)\cdot b(x)=\sum_{i=0}^{m-1}r_i x^i,\quad r_i\in GF(3)$

```
r(x) ← 0
for i = m-1 to 0 do
    r'(x) ← a_i·b(x) + r'(x)·x mod f(x)
end for
r(x) ← r'(x) +b_t·x^t*a(x) mod f(x)
```

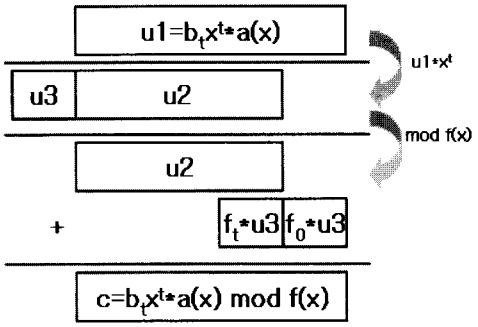


그림 2. $a_t\cdot x^t * b(x)$ mod f(x)의 추가 연산
Fig. 2. The architecture of $a_t\cdot x^t * b(x)$ mod f(x).

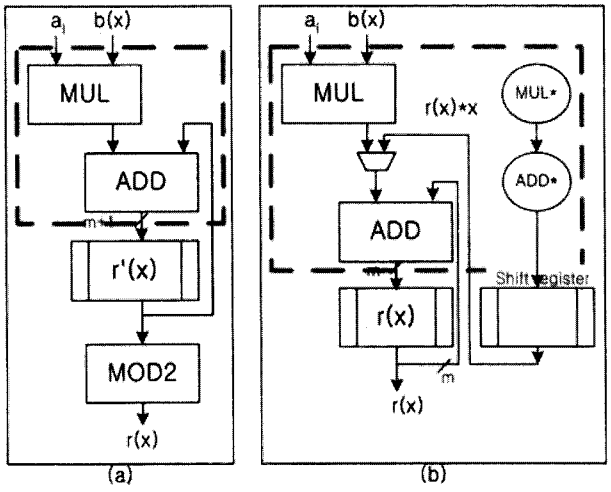


그림 3. 새로운 비트-직렬 곱셈기: (a) 타입 1 (b)타입 2
Fig. 3. New Bit-Serial Multiplier: (a) Type 1 (2) Type 2.

$b'(x)=b(x)-b_t\cdot x^t$라 하면, a(x), b(x)의 곱은 다음과 같다.

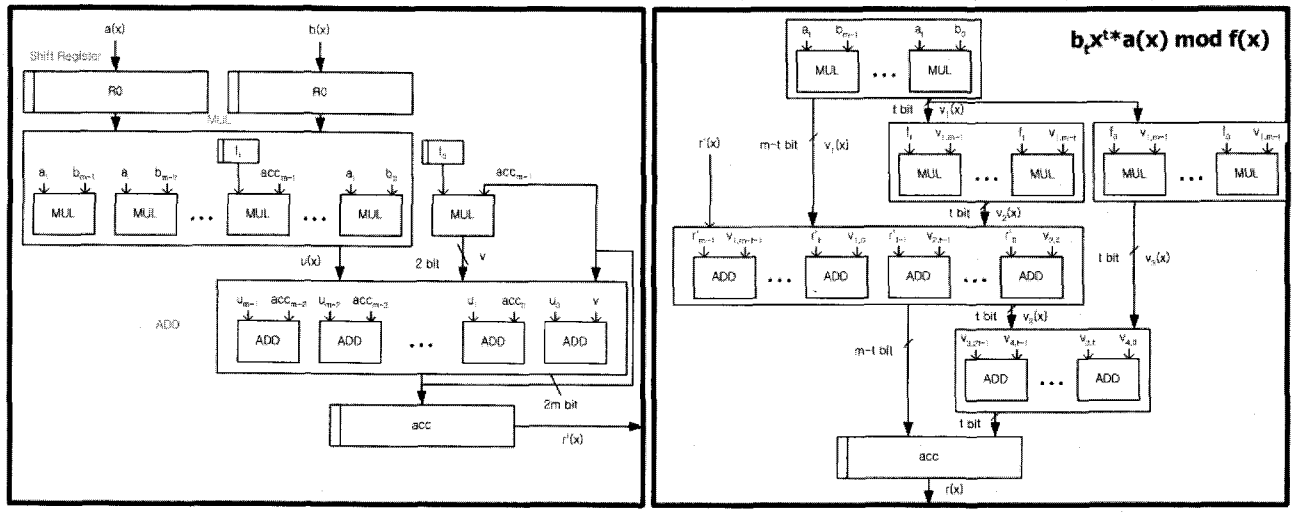


그림 4. GF(3^m) 위의 새로운 타입 1 비트-직렬 곱셈기의 구조
Fig. 4. The architecture ofn new Type 1 Bit-Serial Multiplier over GF(3^m).

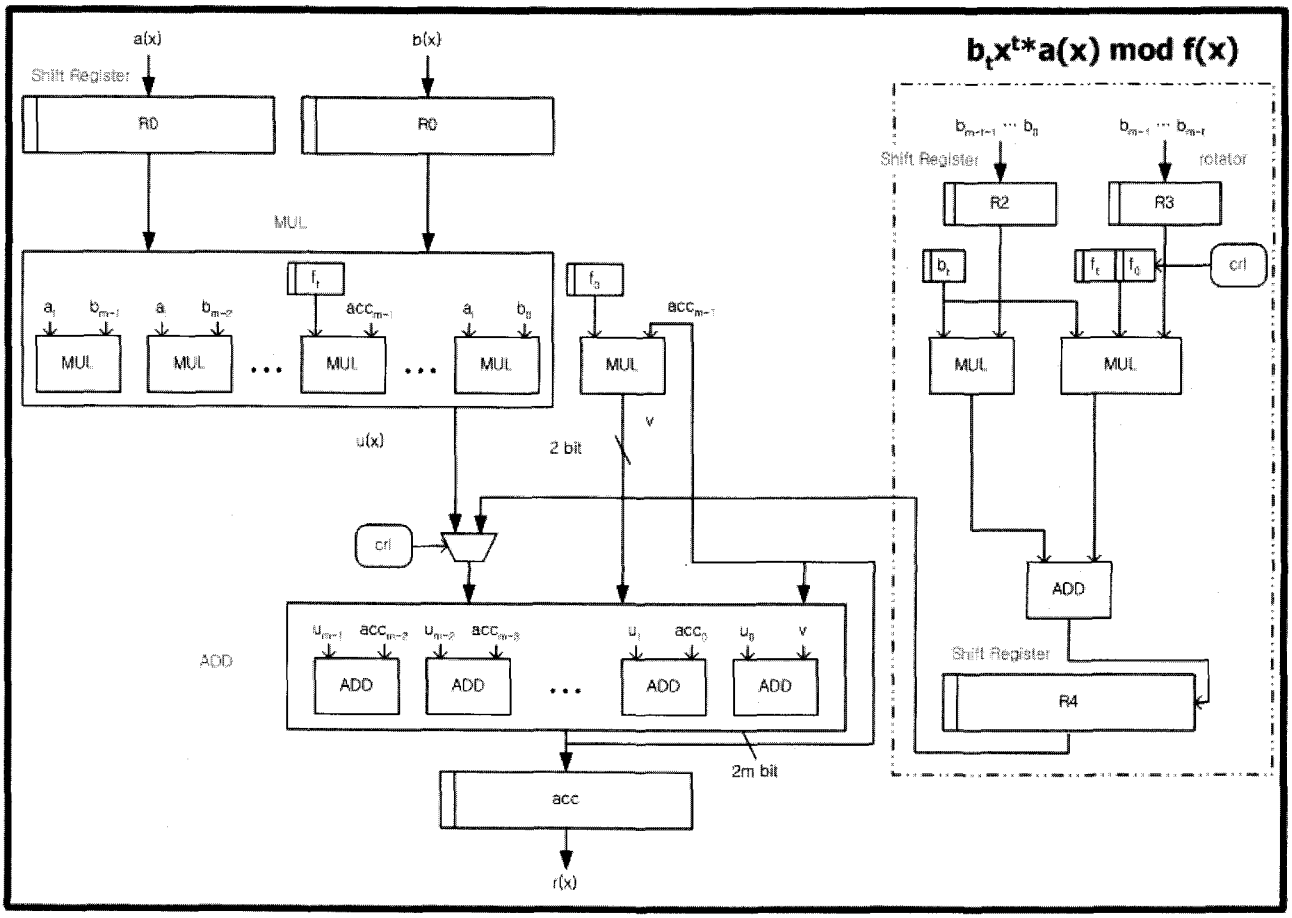


그림 5. GF(3^m) 위의 새로운 타입 2 비트-직렬 곱셈기의 구조
Fig. 5. The architecture ofn new Type 2 Bit-Serial Multiplier over GF(3^m).

$$
\begin{aligned}
&a(x)*b(x) \bmod f(x)\\
&\quad = a(x)*\{b'(x) + b_t\cdot x^t\} \bmod f(x)\\
&\quad = \{a(x)*b'(x) \bmod f(x)\}\\
&\qquad + \{b_t\cdot x^t * a(x) \bmod f(x)\}.
\end{aligned}
$$

이때, 위의 곱셈 방법과 삼항 기약다항식 환경을 고려하면 $a(x)*b'(x) \bmod f(x)$의 연산은 비트-병렬 곱셈기에서 $a_i\cdot b(x)+r'(x)\cdot x \bmod f(x)$ 연산을 반복 수행하게 되며, 이는 다음과 같다.

표 1. 비트-직렬 곱셈기의 복잡도 비교
Table 1. Comparison of Bit-Serial multipliers.

곱셈기		공간 복잡도			시간 복잡도				
		MUL	ADD	Register	MUL	ADD	Critical Path	Iteration	Time Delay
기존 타입 1	곱 셈	m	m-1	4m	1	1	1MUL+1ADD	m	mMUL+mADD
	모듈러	2m+2t-4	2m+t-3	m	2	3	2MUL+3ADD	1	2MUL+3ADD
	합 계	3m+2t-4	3m+t-4	5m	-	-	-	-	(m+2)MUL+(m+3)ADD
기존 타입 2	곱 셈	m+2	m	3m	1	2	1MUL+2ADD	m	mMUL+2mADD
새로운 타입 1	곱 셈	m+2	m	3m	1	1	1MUL+1ADD	m	mMUL+mADD
	모듈러	m+2t	m+t	m	2	3	2MUL+2ADD	1	2MUL+2ADD
	합 계	2m+2t+2	2m+t	4m	-	-	-	-	(m+2)MUL+(m+2)ADD
새로운 타입 2	곱 셈	m+3	m+1	4m	1	1	1MUL+1ADD	m+1	(m+1)MUL+(m+1)ADD

$$a_i \cdot b'(x)+r'(x)\cdot x \bmod f(x)$$
$$= a_i \cdot b'(x)+r'(x)\cdot x - r_{m-1}\cdot f(x)$$
$$= a_i \cdot b(x)+r'(x)\cdot x - r_{m-1}\cdot\{x^m+f_t x^t+f_0\}.$$

위의 식에서 $a_i \cdot b'(x)$는 t항이 없으며, $r'(x)\cdot x$는 상수항이 없으므로 한 번의 덧셈(뺄셈)으로 연산이 가능하다. 따라서 Algorithm 2에 비하여 덧셈 한번으로 고속 연산이 가능하며, 모듈러 연산을 수행하므로 Algorithm 1에 비하여 작은 저장 공간을 사용한다. 이를 정리하면 Algorithm 3과 같다. 또한 추가 모듈러 연산부의 동작 원리는 그림 2과 같다.

Algorithm 3 기반의 곱셈기를 새로운 타입1 곱셈기라 하고, 이는 Algorithm 2 기반의 곱셈기 보다 모듈러 감산부가 추가로 필요하다. 그리고 모듈러 감산부의 복잡도는 유한체 표수에 의존한다. 따라서 추가 모듈러 연산부를 곱셈기 내부에 직렬로 구성하여 설계한 곱셈기 또한 제안한다. 이를 새로운 타입2 곱셈기라 한다. 제안하는 곱셈기는 두 가지 타입으로 Algorithm 3 기반의 연산기의 경우 그림 3(a)와 같으며 추가 모듈러 연산부를 곱셈기 내부에 직렬로 구성한 곱셈기의 경우 그림 3(b)과 같다. 그림 3(a)의 MOD2는 $r'(x)+b_t\cdot x^t\cdot a(x)$의 연산부이며 세부구조는 그림 4와 같다. 그림 3(b)의 MUL*, ADD*은 그림 3(a)의 MOD2를 직렬로 설계한 부분이며 각각 2개, 1개의 계수 연산 모듈로 구성된다. 자세한 세부구조는 그림 5와 같다.

Ⅳ. 비교 및 결론

본 장에서는 제안하는 곱셈기와 기존의 곱셈기의 시간-공간 복잡도 측면의 효율성을 비교하며 비교 결과는 표 1과 같다. 제안하는 곱셈기는 삼항 기약다항식 기반으로 정의되며, 기존의 곱셈기에 비하여 시간 복잡도면에서는 모두 효율적이고, Interleaved 곱셈기의 m·MUL+2m·ADD 시간지연 보다 작은 (m+1)·MUL+(m+1)·ADD 시간지연만으로 수행이 가능하다. 따라서 확장체의 표수가 작은 타원곡선 암호 시스템, 페어링 기반의 암호시스템에서 고속 동작가능하며, 표수가 2 또는 3인 경우 기존의 곱셈기 보다 대략 2배 빠르게 동작한다. 따라서 고속 연산이 요구되는 장비에 효율적이다.

참 고 문 헌

[1] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," *CRYPTO 2002*, LNCS 2442, pp.354-368, Springer-Verlag, 2002.

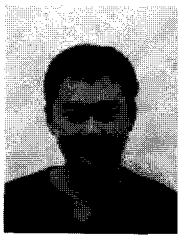
[2] G. Bertoni, J. Guajardo, S. Kumar, G. Orlando C. Paar and T. Wollinger. "Efficient $GF(p^m)$ Arithmetic Architectures for Cryptographic Applications," *CT-RSA 2003*, LNCS 2612, pp.158-175. Springer-Verlag, 2003.

[3] J. Beuchat, M. Shirase, T. Takagi, E. Okamoto, "An Algorithm for the Eta_T Pairing

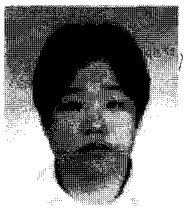
Calculation in Characteristic Three and its Hardware Implementation", *18th IEEE International Symposium on Computer Arithmetic, ARITH-18*, pp.97-104, 2007.
[4] P. Grabher and D. Page, "Hardware Acceleration of the Tate Pairing in Characteristic Three," *CHES 2005*, LNCS 3659, pp.398-411, Springer-Verlag, 2005.
[5] T. Kerins, W. Marnane, E. Popovici, P. S. L. M. Barreto "Efficient Hardware for the Tate Pairing Calculation in Characteristic Three," *CHES 2005*, LNCS 3659, pp.398-411, Springer-Verlag, 2005.
[6] S. Kwon, "Efficient Tate pairing computation for elliptic curves over binary fields," *ACISP 2005*, LNCS 3574, pp.134-145, Springer-Verlag, 2005.
[7] D. Page and N. Smart "Hardware Implementation of Finite Fields of Characteristic Three," *CHES 2002*, LNCS 2523, pp.529-539, Springer-Verlag, 2003.
[8] Koblitz. N, "An Elliptic Curve Implementation of the Finite Field Digital Signature Algorithm", CRYPTO 1998, LNCS 3574, pp. 327-337, Springer-Verlag, 1998.
[9] S. D. Galbraith, "Supersingular Curves in Cryptography", ASIACRYPT 2001, LNCS 2248, pp. 495-513, Springer-Verlag, 2001.

저 자 소 개

장 남 수(학생회원)
2002년 2월 서울시립대학교 수학과 학사.
2004년 8월 고려대학교 정보보호대학원 석사.
2005년~현재 고려대학교 정보경영공학전문대학원 박사과정.
<주관심분야 : 공개키 암호, 암호칩 설계 기술, 부채널 공격 방법론>



이 옥 석(학생회원)
2006년 8월 경원대학교 수학과 학사.
2006년 9월~현재 고려대학교 정보보호대학원 석사과정.
<주관심분야 : 공개키 암호, 암호칩 설계 기술>



김 태 현(학생회원)
2002년 2월 서울시립대학교 수학과 학사.
2004년 8월 고려대학교 정보보호대학원 석사.
2005년~현재 고려대학교 정보경영공학전문대학원 박사과정.
<주관심분야 : 공개키 암호, 부채널 공격, 암호칩 설계 기술>

김 창 한(정회원)
1985년 2월 고려대학교 수학과 학사
1987년 2월 고려대학교 수학과 석사
1992년 2월 고려대학교 수학과 박사
<주관심분야 : 정수론, 공개키암호, 암호프로토콜>